

# IB112 Základy matematiky

## Základy matematické logiky

Jan Strejček

## ■ *Výroková logika*

- výrokové formule, pravdivostní ohodnocení a valuace
- pravdivost a splnitelnost
- normální formy
- úplný systém spojek

## ■ *Predikátová logika*

- termy, kvantifikátory, predikátové formule
- interpretace, valuace, pravdivost

# Výroková logika

## Výroky

- = tvrzení
- = oznamovací věty, u které můžeme určit její pravdivost
- *složený výrok* je poskládán z *atomických výroků* a *spojek*
- Příklady:
  - venku prší (atomický výrok)
  - jestli budeš do osmi v pyžamu, tak bude pohádka (složený výrok)
- Výroky budeme označovat velkými písmeny  $A, B, C, \dots$

## Výroková logika

- Popisuje, jak lze z výroků a logických spojek budovat další výroky.
- Zkoumá vztahy mezi pravdivostmi různých výroků.

## Logické spojky

- = výrazy, kterými z výroků vyrábíme složené výroky
- Příklady: “není pravda, že  $A$ ”, “ $A$ , ledaže by  $B$ ”
- V matematické logice používáme jen vybrané spojky, jejichž význam se může mírně lišit od významu v běžném jazyce. Např. “půjdu tam dnes nebo tam půjdu zítra” chápeme tak, že nastane jen jedna eventualita.

notace	výraz v češtině	název
$\neg A$	“není pravda, že $A$ ”	<i>negace</i>
$A \wedge B$	“ $A$ a $B$ ”	<i>konjunkce</i>
$A \vee B$	“ $A$ nebo $B$ ”	<i>disjunkce</i>
$A \Rightarrow B$	“jestliže $A$ , tak $B$ ”	<i>implikace</i>
$A \Leftrightarrow B$	“ $A$ právě tehdy, když $B$ ”	<i>ekvivalence</i>

- Výrokové formule mohou obsahovat pouze výrokové symboly (reprezentují výroky), logické spojky a závorky (, ).

## Definice (Výrokové formule)

Nechť  $P = \{a, b, c, \dots\}$  je neprázdná množina výrokových symbolů.

*Výrokové formule* nad  $P$  definujeme takto:

- 1 Každá výrokový symbol je výroková formule.
- 2 Jsou-li  $A, B$  výrokové formule, pak i  $(\neg A), (A \wedge B), (A \vee B), (A \Rightarrow B), (A \Leftrightarrow B)$  jsou výrokové formule.
- 3 Nic jiného není výroková formule.

- Výrokové symboly nazýváme *atomické formule*.
- Ostatní výrokové formule se nazývají *složené*.

- Příklady výrokových formulí:  $(a \Rightarrow (\neg b))$ ,  $(\neg((\neg a) \vee b))$ ,  $(a \wedge (b \Leftrightarrow (c \Rightarrow \neg a)))$ , ...
- Odvození  $((a \wedge b) \Leftrightarrow (c \Rightarrow (\neg a)))$ :
  - $a, b, c$  jsou formule dle bodu 1.
  - $(a \wedge b)$  a  $(\neg a)$  jsou formule dle bodu 2.
  - $(c \Rightarrow (\neg a))$  je pak také formule dle bodu 2.
  - Konečně  $((a \wedge b) \Leftrightarrow (c \Rightarrow (\neg a)))$  je také formule dle bodu 2.
- Závorky v zápisu formulí často vynecháváme, pokud tím není dotčena jednoznačnost. Např. píšeme  $(a \wedge b) \Leftrightarrow (c \Rightarrow \neg a)$  namísto  $((a \wedge b) \Leftrightarrow (c \Rightarrow (\neg a)))$ .

# Pravdivostní ohodnocení

- Pravdivost výrokové formule závisí pouze na pravdivosti atomických formulí, které se ve formuli vyskytují.
- Pravdivost atomických formulí je dána *pravdivostním ohodnocením*, pravdivost složených formulí je dána *valuací*.

## Definice (Pravdivostní ohodnocení)

*Pravdivostní ohodnocení (neboli interpretace) je funkce  $I : P \rightarrow \{0, 1\}$  přiřazující každé atomické formuli pravdivostní hodnotu 1 (pravda) nebo 0 (nepravda).*

- Pravdivostní hodnoty 1, 0 se někdy také značí  $T, F$ .



## Definice (Valuace)

Nechť  $I$  je pravdivostní ohodnocení. **Valuace**  $I'$  je funkce přiřazující každé výrokové formuli  $A$  pravdivostní hodnotu 1 nebo 0 a splňující:

- Je-li  $A$  atomická formule, pak  $I'(A) = I(A)$ .
- $I'(\neg A) = 1$  pokud  $I'(A) = 0$  a  $I'(\neg A) = 0$  pokud  $I'(A) = 1$ .
- $I'(A \wedge B) = 1$  pokud  $I'(A) = I'(B) = 1$ . Jinak  $I'(A \wedge B) = 0$ .
- $I'(A \vee B) = 0$  pokud  $I'(A) = I'(B) = 0$ . Jinak  $I'(A \vee B) = 1$ .
- $I'(A \Rightarrow B) = 0$  pokud  $I'(A) = 1$  a  $I'(B) = 0$ . Jinak  $I'(A \Rightarrow B) = 1$ .
- $I'(A \Leftrightarrow B) = 1$  pokud  $I'(A) = I'(B)$ . Jinak  $I'(A \Leftrightarrow B) = 0$ .

- Valuace je pravdivostním ohodnocením určena jednoznačně a je jeho rozšířením.
- Valuaci a pravdivostní ohodnocení tedy lze ztotožnit.

## Definice

Výroková formule  $A$  se nazývá

- **pravdivá při ohodnocení  $I$** , jestliže  $I'(A) = 1$ .
- **pravdivá** nebo **tautologie**, psáno  $\models A$ , pokud je pravdivá při všech ohodnoceních.
- **kontradikce**, pokud není pravdivá při žádném ohodnocení.
- **splnitelná**, pokud je pravdivá při nějakém ohodnocení.

Formule  $A, B$  jsou **ekvivalentní**, psáno  $A \equiv B$ , pokud jsou pravdivé při stejných ohodnoceních.

## Příklady

- tautologie:  $a \vee \neg a$ ,  $a \Rightarrow a$ ,  $a \Leftrightarrow \neg\neg a$ ,  $(a \wedge \neg a) \Rightarrow b$
- kontradikce:  $a \wedge \neg a$ ,  $a \Leftrightarrow \neg a$
- ekvivalentní formule:  $a \Rightarrow b \equiv b \vee \neg a$

Je formule  $((a \wedge b) \Leftrightarrow (c \Rightarrow (\neg a)))$  pravdivá při ohodnocení  $I(a) = 1$ ,  $I(b) = 0$ ,  $I(c) = 1$ ?

Je formule  $((a \wedge b) \Leftrightarrow (c \Rightarrow (\neg a)))$  pravdivá při ohodnocení  $I(a) = 1$ ,  $I(b) = 0$ ,  $I(c) = 1$ ?

- $I(a) = 1$ ,  $I(b) = 0$ ,  $I(c) = 1$
- $I(a \wedge b) = 0$
- $I(\neg a) = 0$
- $I(c \Rightarrow (\neg a)) = 0$
- $I((a \wedge b) \Leftrightarrow (c \Rightarrow (\neg a))) = 1$
- Zadaná formule je při daném ohodnocení pravdivá.

Mnohé tautologie mají svoje názvy:

- komutativní zákony:  $(a \wedge b) \Leftrightarrow (b \wedge a)$ ,  $(a \vee b) \Leftrightarrow (b \vee a)$ , ...
- asociativní zákony:  $((a \wedge b) \wedge c) \Leftrightarrow (a \wedge (b \wedge c))$ , ...
- distributivní zákony:  $(a \wedge (b \vee c)) \Leftrightarrow ((a \wedge b) \vee (a \wedge c))$ , ...
- zákon vyloučení třetího:  $a \vee \neg a$
- zákon sporu:  $\neg(a \wedge \neg a)$
- zákon totožnosti:  $a \Rightarrow a$
- zákon dvojí negace:  $a \Leftrightarrow \neg\neg a$
- idempotence:  $(a \wedge a) \Leftrightarrow a$ ,  $(a \vee a) \Leftrightarrow a$
- de Morganovy zákony:  $\neg(a \wedge b) \Leftrightarrow (\neg a \vee \neg b)$ ,  
 $\neg(a \vee b) \Leftrightarrow (\neg a \wedge \neg b)$
- ...

Věta (Věta o implikaci, sémantický modus ponens)

*Pokud platí  $\models A$  a  $\models A \Rightarrow B$ , pak platí  $\models B$ .*

## Důkaz

Sporem. Necht' platí  $\models A$  a  $\models A \Rightarrow B$  a necht'  $B$  není tautologie. Označme  $I$  ohodnocení, v kterém  $B$  není pravdivé, t.j.  $I(B) = 0$ . Jelikož  $A$  je tautologie, platí  $I(A) = 1$ . Dohromady dostáváme  $I(A \Rightarrow B) = 0$  a proto  $A \Rightarrow B$  není tautologie. To je spor. □

# Pravdivostní tabulka

- *Pravdivostní tabulka* zaznamenává pravdivost dané formule (a jejích podformulí) při všech ohodnoceníh.
- Každý řádek tabulky odpovídá jednomu ohodnocení.
- Počet řádků tabulky je  $2^n$ , kde  $n$  je počet různých atomických formulí v dané formuli.

Pravdivostní tabulka  
pro  $(a \Rightarrow b) \Rightarrow c$

$a$	$b$	$c$	$a \Rightarrow b$	$(a \Rightarrow b) \Rightarrow c$
0	0	0	1	0
0	0	1	1	1
0	1	0	1	0
0	1	1	1	1
1	0	0	0	1
1	0	1	0	1
1	1	0	1	0
1	1	1	1	1

- Z pravdivostní tabulky lze dle výsledných pravdivostních hodnot pro danou formuli snadno určit, zda je formule:
  - tautologie - ve všech řádcích je pravdivostní hodnota 1
  - kontradikce - ve všech řádcích je pravdivostní hodnota 0
  - splnitelná - v nějakém řádku je pravdivostní hodnota 1
- Srovnáním dvou pravdivostních tabulek snadno rozhodneme i ekvivalenci formulí.
- Jelikož existuje algoritmus rozhodující zda je výroková formule pravdivá, říkáme, že výroková logika je *rozhodnutelná*.



# Příklad

- Sestrojte pravdivostní tabulku pro formuli  $a \Rightarrow (b \Rightarrow c)$ .
- Rozhodněte, zda je formule tautologie, kontradikce, splnitelná a zda je ekvivalentní formuli  $(a \Rightarrow b) \Rightarrow c$ .

$a$	$b$	$c$	$b \Rightarrow c$	$a \Rightarrow (b \Rightarrow c)$
0	0	0		
0	0	1		
0	1	0		
0	1	1		
1	0	0		
1	0	1		
1	1	0		
1	1	1		

# Příklad

- Sestrojte pravdivostní tabulku pro formuli  $a \Rightarrow (b \Rightarrow c)$ .
- Rozhodněte, zda je formule tautologie, kontradikce, splnitelná a zda je ekvivalentní formuli  $(a \Rightarrow b) \Rightarrow c$ .

$a$	$b$	$c$	$b \Rightarrow c$	$a \Rightarrow (b \Rightarrow c)$
0	0	0	1	1
0	0	1	1	1
0	1	0	0	1
0	1	1	1	1
1	0	0	1	1
1	0	1	1	1
1	1	0	0	0
1	1	1	1	1

# Příklad

- Sestrojte pravdivostní tabulku pro formuli  $a \Rightarrow (b \Rightarrow c)$ .
- Rozhodněte, zda je formule tautologie, kontradikce, splnitelná a zda je ekvivalentní formuli  $(a \Rightarrow b) \Rightarrow c$ .

$a$	$b$	$c$	$b \Rightarrow c$	$a \Rightarrow (b \Rightarrow c)$
0	0	0	1	1
0	0	1	1	1
0	1	0	0	1
0	1	1	1	1
1	0	0	1	1
1	0	1	1	1
1	1	0	0	0
1	1	1	1	1

- Není tautologie ani kontradikce, je splnitelná a není ekvivalentní formuli  $(a \Rightarrow b) \Rightarrow c$ .

# Disjunktivní normální forma (DNF)

- Jelikož je disjunkce asociativní, tedy  $(A \vee B) \vee C \equiv A \vee (B \vee C)$ , píšeme pouze  $A \vee B \vee C$ . Podobně lze psát i  $A \wedge B \wedge C$ .

## Definice (Literál, konjunktivní klauzule, DNF)

*Literál je atomická formule nebo její negace. Konjunktivní klauzule je konjunkce libovolného konečného počtu literálů. Formule  $A$  je v disjunktivní normální formě (DNF), je-li to jedna klauzule nebo disjunkce konečně mnoha konjunktivních klauzulí.*

## Příklady

- literály:  $a, b, \neg a, \neg c$
- konjunktivní klauzule:  $(a \wedge \neg c \wedge b), (\neg a \wedge \neg c \wedge \neg b \wedge d)$
- formule v DNF:  $(a \wedge \neg c \wedge b) \vee (\neg a \wedge \neg c \wedge \neg b \wedge d) \vee (\neg d)$

# Disjunktivní normální forma (DNF)

## Věta

*Ke každé výrokové formuli existuje ekvivalentní formule v DNF.*

Ekvivalentní formule v DNF lze sestavit z pravdivostní tabulky:

- Pro každé ohodnocení, kde je formule pravdivá, přidáme do vytvářené formule v DNF jednu konjunktivní klauzuli, která bude pro každý pravdivý atomický výrok  $a$  obsahovat literál  $a$  a pro každý nepravdivý atomický výrok  $b$  literál  $\neg b$ .
- Není-li formule pravdivá v žádném ohodnocení, pak je to kontradikce a je ekvivalentní kontradikci  $(a \wedge \neg a)$  a ta je v DNF.

$a$	$b$	$(a \Leftrightarrow \neg b)$
1	1	0
1	0	1
0	1	1
0	0	0

## Věta

*Ke každé výrokové formuli existuje ekvivalentní formule v DNF.*

Ekvivalentní formule v DNF lze sestavit z pravdivostní tabulky:

- Pro každé ohodnocení, kde je formule pravdivá, přidáme do vytvářené formule v DNF jednu konjunktivní klauzuli, která bude pro každý pravdivý atomický výrok  $a$  obsahovat literál  $a$  a pro každý nepravdivý atomický výrok  $b$  literál  $\neg b$ .
- Není-li formule pravdivá v žádném ohodnocení, pak je to kontradikce a je ekvivalentní kontradikci  $(a \wedge \neg a)$  a ta je v DNF.

$a$	$b$	$(a \Leftrightarrow \neg b)$
1	1	0
1	0	1
0	1	1
0	0	0

$\rightsquigarrow (a \wedge \neg b)$

# Disjunktivní normální forma (DNF)

## Věta

*Ke každé výrokové formuli existuje ekvivalentní formule v DNF.*

Ekvivalentní formule v DNF lze sestavit z pravdivostní tabulky:

- Pro každé ohodnocení, kde je formule pravdivá, přidáme do vytvářené formule v DNF jednu konjunktivní klauzuli, která bude pro každý pravdivý atomický výrok  $a$  obsahovat literál  $a$  a pro každý nepravdivý atomický výrok  $b$  literál  $\neg b$ .
- Není-li formule pravdivá v žádném ohodnocení, pak je to kontradikce a je ekvivalentní kontradikci  $(a \wedge \neg a)$  a ta je v DNF.

$a$	$b$	$(a \Leftrightarrow \neg b)$
1	1	0
1	0	1
0	1	1
0	0	0

$$\rightsquigarrow (a \wedge \neg b)$$

$$\rightsquigarrow (\neg a \wedge b)$$

# Disjunktivní normální forma (DNF)

## Věta

Ke každé výrokové formuli existuje ekvivalentní formule v DNF.

Ekvivalentní formule v DNF lze sestavit z pravdivostní tabulky:

- Pro každé ohodnocení, kde je formule pravdivá, přidáme do vytvářené formule v DNF jednu konjunktivní klauzuli, která bude pro každý pravdivý atomický výrok  $a$  obsahovat literál  $a$  a pro každý nepravdivý atomický výrok  $b$  literál  $\neg b$ .
- Není-li formule pravdivá v žádném ohodnocení, pak je to kontradikce a je ekvivalentní kontradikci  $(a \wedge \neg a)$  a ta je v DNF.

$a$	$b$	$(a \Leftrightarrow \neg b)$
1	1	0
1	0	1
0	1	1
0	0	0

$$\rightsquigarrow (a \wedge \neg b)$$

$$\rightsquigarrow (\neg a \wedge b)$$

Celkem:

$$(a \Leftrightarrow \neg b) \equiv$$

$$(a \wedge \neg b) \vee (\neg a \wedge b)$$



# Konjunktivní normální forma (CNF)

- Definice CNF je analogická definici DNF, akorát konjunkce a disjunkce se prohodí.

## Definice (klauzule, CNF)

*(Disjunktivní) klauzule je disjunkce libovolného konečného počtu literálů. Formule  $A$  je v konjunktivní normální formě (CNF), je-li to jedna klauzule nebo konjunkce konečně mnoha klauzulí.*

## Příklady

- klauzule:  $(a \vee \neg c \vee b)$ ,  $(\neg a \vee \neg c \vee \neg b \vee d)$
- formule v CNF:  $(a \vee \neg c \vee b) \wedge (\neg a \vee \neg c \vee \neg b \vee d) \wedge (\neg d)$

# Konjunktivní normální forma (CNF)

## Věta

*Ke každé výrokové formuli existuje ekvivalentní formule v CNF.*

Ekvivalentní formule v CNF lze sestavit z pravdivostní tabulky:

- Pro každé ohodnocení, kde je formule nepravdivá, přidáme do vytvořené formule v CNF jednu klauzuli, která bude pro každý **nepravdivý** atomický výrok  $a$  obsahovat literál  $a$  a pro každý **pravdivý** atomický výrok  $b$  literál  $\neg b$ .
- Je-li formule pravdivá při všech ohodnoceních, je to tautologie a je ekvivalentní tautologii  $(a \vee \neg a)$  a ta je v CNF.

$a$	$b$	$(a \Leftrightarrow \neg b)$
1	1	0
1	0	1
0	1	1
0	0	0

# Konjunktivní normální forma (CNF)

## Věta

*Ke každé výrokové formuli existuje ekvivalentní formule v CNF.*

Ekvivalentní formule v CNF lze sestavit z pravdivostní tabulky:

- Pro každé ohodnocení, kde je formule nepravdivá, přidáme do vytvořené formule v CNF jednu klauzuli, která bude pro každý **nepravdivý** atomický výrok  $a$  obsahovat literál  $a$  a pro každý **pravdivý** atomický výrok  $b$  literál  $\neg b$ .
- Je-li formule pravdivá při všech ohodnoceních, je to tautologie a je ekvivalentní tautologii  $(a \vee \neg a)$  a ta je v CNF.

$a$	$b$	$(a \Leftrightarrow \neg b)$
1	1	0
1	0	1
0	1	1
0	0	0

$$\rightsquigarrow (\neg a \vee \neg b)$$

# Konjunktivní normální forma (CNF)

## Věta

*Ke každé výrokové formuli existuje ekvivalentní formule v CNF.*

Ekvivalentní formule v CNF lze sestavit z pravdivostní tabulky:

- Pro každé ohodnocení, kde je formule nepravdivá, přidáme do vytvářené formule v CNF jednu klauzuli, která bude pro každý **nepravdivý** atomický výrok  $a$  obsahovat literál  $a$  a pro každý **pravdivý** atomický výrok  $b$  literál  $\neg b$ .
- Je-li formule pravdivá při všech ohodnoceních, je to tautologie a je ekvivalentní tautologii  $(a \vee \neg a)$  a ta je v CNF.

$a$	$b$	$(a \Leftrightarrow \neg b)$
1	1	0
1	0	1
0	1	1
0	0	0

$$\rightsquigarrow (\neg a \vee \neg b)$$

$$\rightsquigarrow (a \vee b)$$

# Konjunktivní normální forma (CNF)

## Věta

Ke každé výrokové formuli existuje ekvivalentní formule v CNF.

Ekvivalentní formule v CNF lze sestavit z pravdivostní tabulky:

- Pro každé ohodnocení, kde je formule nepravdivá, přidáme do vytvořené formule v CNF jednu klauzuli, která bude pro každý **nepravdivý** atomický výrok  $a$  obsahovat literál  $a$  a pro každý **pravdivý** atomický výrok  $b$  literál  $\neg b$ .
- Je-li formule pravdivá při všech ohodnoceních, je to tautologie a je ekvivalentní tautologii  $(a \vee \neg a)$  a ta je v CNF.

$a$	$b$	$(a \Leftrightarrow \neg b)$
1	1	0
1	0	1
0	1	1
0	0	0

$$\rightsquigarrow (\neg a \vee \neg b)$$

$$\rightsquigarrow (a \vee b)$$

Celkem:

$$(a \Leftrightarrow \neg b) \equiv$$

$$(\neg a \vee \neg b) \wedge (a \vee b)$$

- Význam výrokových formulí lze také definovat pomocí *pravdivostních funkcí*.

## Definice (Pravdivostní funkce)

*Pravdivostní funkce arity  $n$  je funkce  $f : \{0, 1\}^n \rightarrow \{0, 1\}$ .*

- Pravdivostní funkce každé  $n$ -tici pravdivostních hodnot přiřadí jednu pravdivostní hodnotu.
- Každá formule s  $n$  (uspořádanými) atomickými formulemi jednoznačně určuje pravdivostní funkci arity  $n$ .
- Např.  $a \wedge b$  odpovídá binární pravdivostní funkci  $f(x, y) = x \cdot y$ .

- Pravdivostní funkci lze zapsat tabulkou.

$x$	$y$	$z$	$f(x, y, z)$
0	0	0	0
0	0	1	0
0	1	0	1
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	0

- Lze každou pravdivostní funkci vyjádřit pomocí výrokové formule?

- Pravdivostní funkci lze zapsat tabulkou.

$x$	$y$	$z$	$f(x, y, z)$
0	0	0	0
0	0	1	0
0	1	0	1
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	0

- Lze každou pravdivostní funkci vyjádřit pomocí výrokové formule?
- Ano. Formuli sestojíme z tabulky stejně, jako jsme z tabulky vytvořili formuli v DNF (nebo CNF).



## Definice (Úplný systém spojek)

Množinu logických spojek nazveme **úplný systém spojek**, pokud lze každou pravdivostní funkci vyjádřit pomocí výrokové formule používající pouze spojky z dané množiny.

- Jelikož lze každou pravdivostní funkci popsat formulemi v DNF i v CNF, je množina  $\{\wedge, \vee, \neg\}$  úplným systémem spojek.
- Protože platí  $A \wedge B \equiv \neg(\neg A \vee \neg B)$  lze každou konjunkci vyjádřit pomocí  $\vee, \neg$ . Proto je úplný i systém  $\{\vee, \neg\}$ .
- Podobně  $A \vee B \equiv \neg(\neg A \wedge \neg B)$  a proto je úplný i systém  $\{\wedge, \neg\}$ .
- $\{\Rightarrow, \neg\}$  je také úplný systém.
- Existuje jednoprvkový úplný systém spojek?

$a$	$b$	$a \text{ xor } b$	$a \text{ nand } b$	$a \text{ nor } b$
1	1	0	0	0
1	0	1	1	0
0	1	1	1	0
0	0	0	1	1

- *XOR - exclusive or*,  $A \text{ xor } B \equiv \neg(A \Leftrightarrow B)$
- *NAND - Shefferova funkce*,  $A \text{ nand } B \equiv \neg(A \wedge B)$
- *NOR - Nicodova funkce*,  $A \text{ nor } B \equiv \neg(A \vee B)$
- $\{\text{nand}\}$  i  $\{\text{nor}\}$  tvoří úplné jednoprvkové systémy spojek.
- Všechny tři spojky jsou v informatice významné.

## Definice (Splnitelnost, model, vyplývání)

Nechť  $T$  je množina výrokových formulí. Množina  $T$  je **splnitelná**, pokud existuje ohodnocení, při kterém jsou pravdivé všechny formule z  $T$ . Takové ohodnocení se nazývá **model** množiny  $T$ .

Formule  $A$  **logicky vyplývá** z množiny  $T$ , psáno  $T \models A$ , pokud je  $A$  pravdivá v každém modelu množiny  $T$ .

- $T \models A$  také čteme jako  $A$  je **logickým důsledkem**  $T$ .
- Z nesplnitelné množiny  $T$  vyplývá libovolná formule.
- Splnitelnost konečné množiny formulí  $T$  lze rozhodnout pomocí pravdivostní tabulky obsahující sloupce pro všechny formule z  $T$ . Platnost  $T \models A$  lze rozhodnout analogicky.

# Příklad

Zjistěte, zda je množina formulí  $T = \{\neg b \vee a, \neg a \vee c\}$  splnitelná a zda je jejím důsledkem formule  $b \Rightarrow c$ .

$a$	$b$	$c$	$\neg b \vee a$	$\neg a \vee c$	$b \Rightarrow c$
0	0	0			
0	0	1			
0	1	0			
0	1	1			
1	0	0			
1	0	1			
1	1	0			
1	1	1			

# Příklad

Zjistěte, zda je množina formulí  $T = \{\neg b \vee a, \neg a \vee c\}$  splnitelná a zda je jejím důsledkem formule  $b \Rightarrow c$ .

$a$	$b$	$c$	$\neg b \vee a$	$\neg a \vee c$	$b \Rightarrow c$
0	0	0	1	1	
0	0	1	1	1	
0	1	0	0	1	
0	1	1	0	1	
1	0	0	1	0	
1	0	1	1	1	
1	1	0	1	0	
1	1	1	1	1	

- $T$  je splnitelná.

# Příklad

Zjistěte, zda je množina formulí  $T = \{\neg b \vee a, \neg a \vee c\}$  splnitelná a zda je jejím důsledkem formule  $b \Rightarrow c$ .

$a$	$b$	$c$	$\neg b \vee a$	$\neg a \vee c$	$b \Rightarrow c$
0	0	0	1	1	1
0	0	1	1	1	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	1
1	0	1	1	1	1
1	1	0	1	0	0
1	1	1	1	1	1

- $T$  je splnitelná.
- $b \Rightarrow c$  je důsledkem  $T$ .

# Predikátová logika

- Rozšiřuje výrokovou logiku.
- Umožňuje přesněji popsat výrok a díky tomu odvodit logická vyplývání, která ve výrokové logice odvodit nelze:
  - Každý člověk je smrtelný.
  - Sokrates je člověk.
  - Sokrates je smrtelný.
- Výroky označíme postupně  $a, b, c$ . Ve výrokové logice nelze odvodit logické vyplývání  $c$  z  $a, b$ , přestože  $c$  zjevně je důsledkem  $a, b$ .



Jazyk predikátové logiky se skládá z těchto symbolů:

- *proměnné*:  $x, y, z, x_1, x_2, \dots$
- *logické spojky*:  $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow$
- *kvantifikátory*:  $\forall$  (pro všechna),  $\exists$  (existuje)
- *rovnost*:  $=$
- *závorky*:  $(, )$
- *relační* neboli *predikátové symboly*:  $P, Q, R, P_1, P_2, \dots$
- *funkční symboly*:  $f, g, h, f_1, f_2, \dots$
- Každý predikátový symbol má pevně danou aritu  $n > 0$ .
- Každý funkční symbol má pevně danou aritu  $n \geq 0$  (počet argumentů).
- Funkce s aritou 0 se nazývají *konstanty* a značí se  $a, b, c, \dots$

- Konstanty, proměnné i funkce slouží k označení *objektů*.
- Objekty jsou prvky dané množiny objektů nazývané *doména* nebo *univerzum*.
- Konstanty jsou vlastně jména objektů.
- Proměnné zastupují libovolné objekty.
- Pomocí funkcí vytváříme složená jména objektů.

## Příklad

- Uvažujme doménu nezáporných celých čísel.
- Konstanty jsou např.  $0$ ,  $1$ ,  $42$ .
- Příkladem binární funkce (funkce arity 2) je  $+$ .
- Složené jméno objektu  $3$  je například  $1 + 2$  nebo  $(1 + 1) + 1$ .
- Složené jméno objektu je i  $x + 2$  nebo  $(x + 2) + (z + x)$ .

- Termy jsou všechna možná označení objektů.

## Definice (Termy)

*Termy* definujeme takto:

- 1 *Každá proměnná je term.*
- 2 *Je-li  $f$  funkční symbol arity  $n$  a  $t_1, t_2, \dots, t_n$  jsou termy, pak i  $f(t_1, t_2, \dots, t_n)$  je term.*
- 3 *Nic jiného není term.*

- Z bodu (2) plyne, že konstanty (nulární funkce) jsou také termy.
- Příklady termů:  $a, 0, x, f(x, 0, a), f(g(a, 0), 2, h(h(y)))$

- Nulární predikát je výrok (jako ve výrokové logice).
- Unární predikát
  - popisuje vlastnost objektu,
  - odpovídá výroku, ze kterého odstraníme označení jednoho objektu.
  - Příklad: Predikát  $P$  odpovídá pojmu “být smrtelný”
    - “Objekt  $x$  je smrtelný”  $\rightsquigarrow P(x)$
    - “Sokrates je smrtelný”  $\rightsquigarrow P(\text{Sokrates})$
- Binární predikát
  - popisuje vztah mezi dvěma objekty.
  - Příklad: “ $x$  je násobek  $y$ ”  $\rightsquigarrow Q(x, y)$ 
    - “ $x + 3$  je násobek 2”  $\rightsquigarrow Q(x + 3, 2)$
    - “ $x$  je menší než 7”  $\rightsquigarrow x < 7$  (infixová notace)
- Predikát arity  $n$  popisuje vztah mezi  $n$  objekty.

## $\forall$ - univerzální neboli obecný kvantifikátor

- $(\forall x)P(x)$  říká, že pro všechny objekty  $x$  z domény platí  $P(x)$ .
- Pro konečnou doménu  $\{a_1, a_2, \dots, a_n\}$  je  $(\forall x)P(x)$  ekvivalentní formuli  $P(a_1) \wedge P(a_2) \wedge \dots \wedge P(a_n)$ .

## $\exists$ - existenciální kvantifikátor

- $(\exists x)P(x)$  říká, že existuje (alespoň jeden) objekt  $x$  z domény, pro který platí  $P(x)$  (neboli  $P(x)$  platí pro některé objekty  $x$ ).
- Pro konečnou doménu  $\{a_1, a_2, \dots, a_n\}$  je  $(\exists x)P(x)$  ekvivalentní formuli  $P(a_1) \vee P(a_2) \vee \dots \vee P(a_n)$ .

## Příklad

- Nechť  $P$  odpovídá pojmu “být smrtelný”.
- Uvažujme doménu všech lidí.
- $(\forall x)P(x)$  říká, že všichni lidé jsou smrtelní.
- $(\exists x)P(x)$  říká, že existuje smrtelný člověk (neboli někteří lidé jsou smrtelní).

## Definice (Predikátové formule)

*Atomické predikátové formule* definujeme takto:

- 1 Necht'  $P$  je predikátový symbol arity  $n$  a  $t_1, \dots, t_n$  jsou termy. Pak  $P(t_1, \dots, t_n)$  je atomická predikátová formule.
- 2 Jsou-li  $t_1, t_2$  termy, pak  $t_1 = t_2$  je atomická predikátová formule.
- 3 Nic jiného není atomická predikátová formule.

*Predikátové formule* definujeme takto:

- 1 Každá atomická predikátová formule je predikátová formule.
- 2 Jsou-li  $\varphi, \psi$  predikátové formule, pak i  $\neg\varphi, \varphi \vee \psi, \varphi \wedge \psi, \varphi \Rightarrow \psi, \varphi \Leftrightarrow \psi$  jsou predikátové formule.
- 3 Je-li  $x$  proměnná a  $\varphi$  predikátová formule, pak  $(\forall x)\varphi$  a  $(\exists x)\varphi$  jsou predikátové formule.
- 4 Nic jiného není predikátová formule.

## Příklad

- $\mathbb{N}_0$  s elementární aritmetikou: konstanta  $0$ , unární funkce následník  $s$ , binární funkce  $+$ ,  $*$
- termy:  $s(0)$  reprezentuje  $1$ ,  $s(x) + s(s(0))$  reprezentuje  $(x + 1) + 2$
- $(\forall x) 0 * x = 0$  ... nula krát cokoliv je nula
- $(\forall x) s(0) * x = x$  ... jedna krát libovolné číslo je totéž číslo
- $\neg(\exists x) s(x) = 0$  ... v dané doméně nemá nula předchůdce

## Příklad

- Nechť  $R$  je binární predikát reprezentující binární relaci.
- $(\forall x) R(x, x)$  ...  $R$  je reflexivní
- $(\forall x)(\forall y) (R(x, y) \Rightarrow R(y, x))$  ...  $R$  je symetrická
- $(\forall x)(\forall y)(\forall z) ((R(x, y) \wedge R(y, z)) \Rightarrow R(x, z))$  ...  $R$  je tranzitivní

# Vázaný a volný výskyt proměnných

- **Podformule** formule  $\varphi$  je každá souvislá část  $\varphi$ , která je také formulí.
- Podformule  $\psi$  ve formulích  $(\forall x)\psi$  a  $(\exists x)\psi$  se nazývá **oborem** nebo **rozsahem** kvantifikátoru  $(\forall x)$  nebo  $(\exists x)$ .
- Výskyt proměnné  $x$  ve formuli  $\varphi$  je **vázaný**, je-li v rozsahu nějakého kvantifikátoru  $(\forall x)$  nebo  $(\exists x)$ .
- Výskyty, které nejsou vázané, jsou **volné**.
- Příklad:  $((\forall x)(\exists y)P(x, y, z)) \Rightarrow R(x, z)$  ... **vázaný/volný** výskyt
- Proměnná se nazývá **volná** (resp. **vázaná**), existuje-li v dané formuli její **volný** (resp. **vázaný**) výskyt.
- Formule bez volných proměnných se nazývá **sentence** neboli **uzavřená formule**.
- Formule bez kvantifikátorů se nazývá **otevřená formule**.
- Zápis  $\varphi(x_1, x_2, \dots, x_n)$  označuje formuli  $\varphi$  a zdůrazňuje, že všechny volné proměnné formule  $\varphi$  jsou mezi  $x_1, x_2, \dots, x_n$ .



# Sémantika predikátové logiky

K definici sémantiky potřebujeme určit množinu objektů (doménu) a dále dát význam funkčním a predikátovým symbolům. Proměnným je třeba přiřadit objekty.

## Definice (Realizace/interpretace)

*Realizace* neboli *interpretace*  $I$  jazyka predikátové logiky je struktura obsahující

- neprázdnou množinu  $D$  zvanou *doména* nebo *univerzum*,
- funkci  $I(f) : D^n \rightarrow D$  pro každý  $n$ -ární funkční symbol  $f$ ,
- relaci  $I(P) \subseteq D^n$  pro každý  $n$ -ární relační symbol  $P$ .

## Definice (Ohodnocení/valuace proměnných)

*Ohodnocení* neboli *valuace proměnných* je zobrazení  $V$  přiřazující každé proměnné prvek domény  $D$ .

- Uvažme jazyk predikátové logiky obsahující:
  - konstantu  $0$
  - unární funkci  $s$
  - binární funkce  $+, *$
  - binární relaci  $<$
- Standardní interpretace  $I$  tohoto jazyka:
  - doména  $\mathbb{N}_0$
  - $I(0)$  je číslo  $0$
  - $I(s)(n) = n + 1$  pro každé  $n \in \mathbb{N}_0$
  - $I(+), I(*)$  jsou operace sčítání a násobení na  $\mathbb{N}_0$
  - $I(<)$  je relace “menší než” na  $\mathbb{N}_0$
- Nestandardní, ale taky možná interpretace  $I'$ :
  - doména  $D = \{a, b\}$
  - $I'(0)$  je prvek  $a$
  - $I'(s)(a) = b, I'(s)(b) = a$
  - $I'(+)(x, y) = a, I'(*) (x, y) = y$  pro všechna  $x, y \in \{a, b\}$
  - $I'(<) = \{(a, b), (a, a)\}$

## Definice (Hodnota termu)

*Hodnotou termu  $t$  při interpretaci  $I$  a valuaci  $V$  rozumíme prvek  $|t|_{I,V}$  domény  $D$  definovaný dle tvaru termu takto:*

- *Je-li  $t$  proměnná  $x$ , pak  $|t|_{I,V} = V(x)$ .*
- *Je-li  $t$  tvaru  $f(t_1, t_2, \dots, t_n)$ , pak  $|t|_{I,V} = I(f)(|t_1|_{I,V}, |t_2|_{I,V}, \dots, |t_n|_{I,V})$ .*

- Hodnota proměnné je tedy přímo dána valuací této proměnné.
- Hodnotu termu  $f(t_1, t_2, \dots, t_n)$  získáme tak, že vezmeme hodnoty termů  $t_1, t_2, \dots, t_n$  a na tyto hodnoty aplikujeme funkci  $I(f)$  přiřazenou symbolu  $f$  interpretací  $I$ .
- Hodnota termu závisí pouze na valuaci proměnných, které se v termu vyskytují.

## Příklad

Určete hodnotu termu  $s(s(0)) * s(x + s(0))$  při dříve definované interpretaci  $I$  a valuaci  $V(x) = 7$ .

Určete hodnotu termu  $s(s(0)) * s(x + s(0))$  při dříve definované interpretaci  $I$  a valuaci  $V(x) = 7$ .

- $|0|_{I,V} = I(0) = 0$
- $|s(0)|_{I,V} = I(s)(|0|_{I,V}) = I(s)(0) = 0 + 1 = 1$
- $|s(s(0))|_{I,V} = I(s)(|s(0)|_{I,V}) = I(s)(1) = 1 + 1 = 2$
- $|s(x + s(0))|_{I,V} = I(s)(V(x) + 1) = I(s)(7 + 1) = 8 + 1 = 9$
- $|s(s(0)) * s(x + s(0))|_{I,V} = |s(s(0))|_{I,V} \cdot |s(x + s(0))|_{I,V} = 2 \cdot 9 = 18$

Určete hodnotu termu  $s(s(0)) * s(x + s(0))$  při dříve definované interpretaci  $I$  a valuaci  $V(x) = 7$ .

- $|0|_{I,V} = I(0) = 0$
- $|s(0)|_{I,V} = I(s)(|0|_{I,V}) = I(s)(0) = 0 + 1 = 1$
- $|s(s(0))|_{I,V} = I(s)(|s(0)|_{I,V}) = I(s)(1) = 1 + 1 = 2$
- $|s(x + s(0))|_{I,V} = I(s)(V(x) + 1) = I(s)(7 + 1) = 8 + 1 = 9$
- $|s(s(0)) * s(x + s(0))|_{I,V} = |s(s(0))|_{I,V} \cdot |s(x + s(0))|_{I,V} = 2 \cdot 9 = 18$

Totéž při interpretaci  $I'$  a valuaci  $V'(x) = b$ .

Určete hodnotu termu  $s(s(0)) * s(x + s(0))$  při dříve definované interpretaci  $I$  a valuaci  $V(x) = 7$ .

- $|0|_{I,V} = I(0) = 0$
- $|s(0)|_{I,V} = I(s)(|0|_{I,V}) = I(s)(0) = 0 + 1 = 1$
- $|s(s(0))|_{I,V} = I(s)(|s(0)|_{I,V}) = I(s)(1) = 1 + 1 = 2$
- $|s(x + s(0))|_{I,V} = I(s)(V(x) + 1) = I(s)(7 + 1) = 8 + 1 = 9$
- $|s(s(0)) * s(x + s(0))|_{I,V} = |s(s(0))|_{I,V} \cdot |s(x + s(0))|_{I,V} = 2 \cdot 9 = 18$

Totéž při interpretaci  $I'$  a valuaci  $V'(x) = b$ .

- $|s(x + s(0))|_{I',V'} = I'(s)(a) = b$
- $|s(s(0)) * s(x + s(0))|_{I',V'} = b$

# Sémantika predikátové logiky

$V[x/d]$  značí valuaci lišící se od  $V$  pouze tím, že proměnné  $x$  přiřazuje prvek  $d$ .

## Definice (Pravdivost predikátové formule)

Formule  $\varphi$  je **pravdivá při interpretaci  $I$  a valuaci  $V$** , psáno  $I, V \models \varphi$ , pokud  $\varphi$  je tvaru

- $P(t_1, t_2, \dots, t_n)$  a  $(|t_1|_{I,V}, |t_2|_{I,V}, \dots, |t_n|_{I,V}) \in I(P)$ ,
- $t_1 = t_2$  a  $|t_1|_{I,V} = |t_2|_{I,V}$
- $\neg\psi$  a  $I, V \not\models \psi$ ,
- $\psi_1 \vee \psi_2$  a  $I, V \models \psi_1$  nebo  $I, V \models \psi_2$ ,
- $\psi_1 \wedge \psi_2$  a  $I, V \models \psi_1$  a  $I, V \models \psi_2$ ,
- $\psi_1 \Rightarrow \psi_2$  a  $I, V \not\models \psi_1$  nebo  $I, V \models \psi_2$ ,
- $\psi_1 \Leftrightarrow \psi_2$  a  $I, V \models \psi_1$  a  $I, V \models \psi_2$ , nebo  $I, V \not\models \psi_1$  a  $I, V \not\models \psi_2$ ,
- $(\forall x)\psi$  a  $I, V[x/d] \models \psi$  pro každé  $d$  z domény  $D$ ,
- $(\exists x)\psi$  a  $I, V[x/d] \models \psi$  pro nějaké  $d$  z domény  $D$ .



- Snadno se ověří, že pravdivost formule  $\varphi$  při interpretaci  $I$  a valuaci  $V$  záleží pouze na valuaci proměnných, které jsou volné ve  $\varphi$  a na interpretaci symbolů použitých ve formuli  $\varphi$ .
- Z toho okamžitě plyne, že pravdivost sentencí vůbec nazáleží na valuaci.

## Definice

*Predikátová formule  $\varphi$  se nazývá*

- *pravdivá při interpretaci  $I$ , psáno  $I \models \varphi$ , jestliže  $\varphi$  je pravdivá při interpretaci  $I$  a všech valuacích  $V$ .*
- *pravdivá nebo tautologie, psáno  $\models \varphi$ , jestliže je pravdivá při všech interpretacích.*
- *splnitelná, jestliže je pravdivá při nějaké interpretaci.*

Zjistěte, zda je formule  $\varphi = (\forall x) x < s(x)$  splnitelná nebo dokonce tautologie.

Zjistěte, zda je formule  $\varphi = (\forall x) x < s(x)$  splnitelná nebo dokonce tautologie.

- Uvažme dříve uvedené interpretace  $I$  a  $I'$ .
- Formule  $\varphi$  je splnitelná, neboť například  $I \models \varphi$ .
- Formule  $\varphi$  není tautologie, neboť například  $I' \not\models \varphi$  (formule  $x < s(x)$  není pravdivá při  $I'$  a  $V'(x) = b$ ).

Vymyslete nějakou tautologii nad daným jazykem predikátové logiky.

- de Morganovy zákony pro kvantifikátory:

$$\neg(\forall x)\varphi(x) \Leftrightarrow (\exists x)\neg\varphi(x), \quad \neg(\exists x)\varphi(x) \Leftrightarrow (\forall x)\neg\varphi(x)$$

- zaměnitelnost kvantifikátorů stejného typu:

$$(\forall x)(\forall y)\varphi(x, y) \Leftrightarrow (\forall y)(\forall x)\varphi(x, y),$$

$$(\exists x)(\exists y)\varphi(x, y) \Leftrightarrow (\exists y)(\exists x)\varphi(x, y)$$

- distributivita kvantifikátorů:

$$(\forall x)(\varphi(x) \wedge \psi(x)) \Leftrightarrow (\forall x)\varphi(x) \wedge (\forall x)\psi(x),$$

$$(\exists x)(\varphi(x) \vee \psi(x)) \Leftrightarrow (\exists x)\varphi(x) \vee (\exists x)\psi(x)$$

- redukce univerzálního kvantifikátoru:

$$(\forall x)(\forall y)\varphi(x, y) \Rightarrow (\forall y)\varphi(y, y)$$

- $(\forall x)\varphi(x) \Rightarrow (\exists x)\varphi(x)$

- ...

## Definice (Teorie, model, důsledek)

Množina sentencí  $T$  se nazývá **teorie**. Interpretace  $I$  se nazývá **model** teorie  $T$ , jestliže  $I \models \varphi$  pro každé  $\varphi \in T$ . Formule  $\psi$  **logicky vyplývá** z teorie  $T$  ( $\psi$  je **důsledkem**  $T$ ), psáno  $T \models \psi$ , pokud je  $\psi$  pravdivá v každém modelu teorie  $T$ . Teorie  $T$  je **sporná**, pokud nemá žádný model. V opačném případě je teorie **bezesporná**.

## Příklad

- Formální zápis Sokratovy úvahy:

$$\{(\forall x)(C(x) \Rightarrow S(x)), C(\text{Sokrates})\} \models S(\text{Sokrates})$$

- V predikátové logice prvního řádu lze kvantifikovat pouze přes proměnné.
- V logice druhého řádu lze kvantifikovat i přes predikátové symboly.